Compliance Manual is updated to account for any changes in law relating to CPNI. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company trains its personnel for compliance with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods for telephone access, online access, and in-store access to CPNI, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters." In-store visits require valid photo identification.

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has not encountered any circumstances requiring it to take any action against a data broker during the year to which this Certificate pertains. [Or: The Company has taken the following actions against data brokers: list case name, docket or case number, and name of data broker.]

Summary of all Customer Complaints Received

15. The following is a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI: None. [Or: list number of customer complaints received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, e.g., improper access by employees, improper disclosure to individuals not authorized to receive the information, or improper access to online information by individuals not authorized to view the information.]

16. The Company does not at this point have any specific information on the processes pretexters are using to attempt to access its Customer's CPNI. [Or, explain specific information the company has regarding the processes pretexters are using to attempt to access CPNI, and what steps it is taking to protect CPNI. If the Company has information to provide on this topic, it should submit both redacted and un-redacted versions of this form to the FCC.]

The company represents and warrants that this certification is consistent with 47 CFR 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Date: _____ _____

APPENDIX 2

EMPLOYEE VERIFICATION OF CPNI MANUAL REVIEW

Employee Verification

Employee Name (*Please print*):

I have reviewed the Company's Customer Proprietary Network Information (CPNI) Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

I am also aware that any violation of the Company's CPNI Operating Procedures is subject to the disciplinary procedure set forth in the Hiawatha Communications Inc. Employee Handbook (*Section(s) 401,401(a), 401(b); Page(s) IV-1, IV-2*).

_____

Employee Signature

_____

Date

APPENDIX 3A

SAMPLE Customer CPNI PIN and Password Setup Request Notification

OCTC
ONTONAGON COUNTY TELCO

www.ontonagon-telephone.com

618 RIVER STREET ONTONAGON, MI 49953 (906) 884-9911 or 1-800-562-7113 FAX (906) 884-6450

Customer Action Required

Date:

John Sample
12345 Any Street
Anytown, MI 00012

Account Number: ##########
Unique PIN: 123456

Dear Customer Name:

At OCTC, the privacy and security of your account is very important to us. This is why we fully comply with the federal laws and FCC regulations that require proper authentication of our customers prior to disclosing private account information.

To better protect all of your account information and allow us to provide you the best quality customer service, the FCC now requires that you establish a password, as well as two backup security questions to use in the event you forget your password, as soon as possible in order to access your OCTC account. **At your earliest convenience, please call our local office at (906) 884-9911 or stop by our local office located at 618 River Street, Ontonagon, MI to set up your password and responses to the security questions.** Our office hours are 8:00 AM – 5:00 PM Monday-Friday. In order to access your account to establish the secure password and security questions, you will need your account number and the unique PIN (Personal Identification Number) listed at the top of this letter.

Please be advised you must have a password (not just the unique PIN above) created by 12/31/07. Due to recent changes in the Federal Communications Commission's rules governing customer privacy (CPNI), OCTC will be implementing its new password policy effective December 10, 2007. Failure to do so will severely diminish the amount of information we will be able to divulge to you regarding your account and will also limit the types of transactions you may complete online or over the phone. For your convenience, we have provided answers to frequently

asked questions on our website, www.jamadots.com, to provide additional information on this very important and mandatory change.

Thank you in advance for completing this request as soon as possible. Your protection is our priority and we need your help to complete this very important task.

Sincerely,

OCTC Management

APPENDIX 3B

SAMPLE OPT-OUT NOTICE

Date: _____

PROTECTING YOUR PRIVACY

Ontonagon County Telephone Company. (OCTC) protects the confidentiality of its telecommunications customers consistent with applicable law, including the FCC's regulations governing Customer Proprietary Network Information (CPNI).

What Is CPNI?

CPNI is information OCTC obtains or creates in the normal course of providing local or long distance telecommunications services to you. This information includes the quantity and types of telecommunications services you currently receive, how you use them and related billing information, such as call destination, location and amount of use. CPNI is made available to OCTC solely by virtue of our carrier-customer relationship. CPNI does not include your telephone number, name and address since this information is typically published in a telephone directory.

What Can OCTC Do With CPNI?

OCTC is permitted to use CPNI to provide the telecommunications services you purchase, including billing and collections for those services. OCTC can also use or disclose CPNI, without your approval, to offer enhancements to telecommunications services of the same type that you already purchase from us. For example, if you purchase basic local telephone services, OCTC does not need your approval to use your customer information to offer you enhanced services such as voicemail or caller ID services.

OCTC is also permitted by federal law to use, disclose, or permit access to your individually identified customer information in certain circumstances: (1) as required by law or court order; (2) with your approval; (3) in providing or marketing the services from which the customer information is derived or services necessary to or used in such services; (4) to initiate, render, bill and collect for services; (5) for the provisioning of inside wiring, installation, maintenance and repair services; or (6) to investigate fraud or to protect against unlawful or abusive use of service and to protect other users.

Examples where disclosure of CPNI is permitted without your approval:
• When you dial 911, information about your location may be transmitted automatically to a public safety agency.

• Certain information about your long distance calls is transmitted to your long distance company for billing purposes.
• We must disclose information, as necessary, to comply with court orders or subpoenas.
• We also will share information to protect its rights or property and to protect users of its services and other carriers from
fraudulent, abusive or unlawful use of services.
• We may, where permitted by law, provide information to credit bureaus, or provide information and or sell receivables
to collection agencies to obtain payment for OCTC billed products and services.

OCTC may also use, disclose or permit access to your customer information for the marketing of different categories of service to which you do not subscribe. However, we must obtain your approval to do so.

Disclosure of CPNI

Protecting the confidentiality of your CPNI is your right and OCTC's duty under federal law. We do not sell or disclose CPNI to anyone outside of OCTC or to anyone not authorized to represent us to offer products or services, or to perform functions on our behalf, except as may be required or permitted by law or authorized by you. When OCTC uses agents, contractors or other companies to perform services on our behalf, we require them to protect your CPNI consistent with applicable law. OCTC does not disclose CPNI to any unaffiliated third parties for use in their own marketing.

Notice of Your Rights to Restrict CPNI

You have the right under federal law to restrict our use or disclosure of and access to your CPNI. You also have the right to grant or deny access to your CPNI. This Notice seeks your consent to permit OCTC to use, disclose or permit access to your CPNI for purposes of marketing other communications-related service offerings to which you do not already subscribe. Your approval will be deemed granted unless you otherwise notify us. At no time will your decision to deny approval affect the provision of any telecommunications services from OCTC. However, without your approval, our ability to provide you with information on other services will be prohibited.

Restricting Our Use of CPNI

No action by you is necessary to permit us to access and use your CPNI information to offer you communications related services that may be different from the type of services you currently receive. Your approval to use CPNI may enhance OCTC's ability to offer products and services tailored to your needs. You have 35 days from the date of this Notice to advise us if you DO NOT want us to use your CPNI for this purpose before approval is assumed. Only OCTC and its authorized representatives will use the CPNI. You may inform us of your decision to deny access by either calling our office, in writing or by e-mail as set forth below. There is no cost to you for your decision. After the 35 days has expired, OCTC may begin using your information to offer different products to you. At any time after the 35 days, however, you can change your decision by contacting us. You have

the right to disapprove, and revoke or limit access to your CPNI at any time and at no cost. Your decision will remain effective until you change it.

How To Contact OCTC

Written: OCTC, Attn: Subscriber Privacy, 618 River Street, Ontonagon, MI 49953
Telephone: (906) 884-9911 or Toll Free (800) 562-7113
E-mail: OCTCcpni@jamadots.com
Telephone and e-mail are available 24 hours a day, seven days a week to allow you to opt-out whenever you choose. If you call at a time other than our regular business hours please leave a message. We will follow-up with you for confirmation of the information the following business day.

Additional information on CPNI privacy is available from the FCC via the Internet at:
http://www.fcc.gov/cgb/complaints.html
Telephone
Voice: 1-888-CALL-FCC (1-888-225-5322)
TTY: 1-888-TELL-FCC (1-888-835-5322)
Mail:
Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, DC 20554

APPENDIX 4

SAMPLE FORM FOR DISCLOSURE OF CPNI TO THIRD PARTY ON CUSTOMER'S REQUEST

Customer Proprietary Network Information
Grant of Permission to Disclose CPNI to Third Party

Pursuant to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (subpart U of Part 64 of the FCC Rules), Ontonagon County Telephone Company is unable to provide any information regarding your account to any other party without your express written permission to do so.

Your Account Billing Name _____

Your Account Billing Address _____

Your Billing Telephone Number(s) _____

I give my written permission to allow _____,
whose address is _____,
whose phone number is_____,

to receive written, and/or electronic responses for the following information on the above stated account (describe):

Signature:_____

Printed Name_____

Date:_____

You may revoke this Grant of Permission by writing to us at:

or calling us at:

For Company Use:

Customer did one of the following:

☐ Requested Call Detail Information, presented a Valid Photo ID, and established a password.
☐ Requested Call Detail Information, and provided password.
☐ Requested CPNI other than Call Detail Information, and provided password.
☐ Requested CPNI other than Call Detail Information, and presented a Valid Photo ID.
☐ Requested CPNI other than Call Detail Information, and was authenticated by a Company representative calling the Customer's Telephone Number of Record.

APPENDIX 5

Log of Customer Complaints Related to CPNI

LOG OF CUSTOMER COMPLAINTS RELATED TO CPNI

Affected Customer Name	Date of Compliant	Description of Complaint

Red Flag Rules Manual

Red Flags and Address Discrepancies

Compliance Manual and Operating Procedures

For

Hiawatha Telephone Company
Chippewa County Telephone Company
Ontonagon County Telephone Company
Midway Telephone Company

October 2008

TABLE OF CONTENTS

SECTION 1

DEFINITIONS

Account: A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

Annual Report: See Section 9.

Board of Directors: The Company's board of directors, or if the Company does not have a board of directors, a designated employee at the level of senior management.

Covered Account: An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Telecommunication service accounts can be Covered Accounts. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

Company: Hiawatha Company's

SECTION 1

DEFINITIONS (CONT'D)

Consumer Report: A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 *et seq.*

Credit: The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

Creditor: A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit. Telecommunication service providers can be Creditors.

Customer: A person that has a Covered Account with a Creditor or a financial institution.

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

SECTION 1

DEFINITIONS (CONT'D)

Identifying Information: A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

Notice of Address Discrepancy: A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

Red Flag: See Section 3.

Readily Available Biographical Information: Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

Service Provider: A provider of a service directly to a financial institution or Creditor.

SECTION 2

STATEMENT OF CORPORATE POLICY

The policy of Hiawatha Company's is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 *et seq.*, and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to Jay Brogan, President and C.E.O.

- The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:

  Jay Brogan, President and C.E.O.

- The Company's Board of Directors Approved this Manual on April 9, 2009.

SECTION 3

WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents.
- Unusual use or suspicious activity related to a Covered Account.
- Presentation of suspicious personal identification information.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

SECTION 4

IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts, taking into consideration:

- The methods of opening Accounts;
- The methods of access to Accounts; and
- Previous experiences with Identity Theft.

SECTION 5

OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);

2. Detect Red Flags (see Section 6);

3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and

4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

SECTION 6

IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not open a Covered Account or provide any service until it is able to satisfactorily identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the opening of the Covered Account on hold until it can satisfactorily resolve the Red Flag.